UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,550	08/16/2001	Steven Dale Goodman	RPS9 2001 0042	3291

45211 7590 02/07/2006

KELLY K. KORDZIK
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 02/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/931,550
Filing Date: August 16, 2001
Appellant(s): GOODMAN ET AL.

Kelly K. Kordzik
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 21 November 2005 appealing from the Office action mailed 28 July 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

(3) Status of Claims

The statement of the status of claims contained in the brief is substantially correct. Claims 3-5, 7-9, 12-14, and 16-18 stand rejected. The changes are as follows: Claim 19 is allowed. Claims 6 and 15 are objected to as allowable but dependent upon a rejected base claim.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Alexander et al US Patent No. 6,188,602.

Grawrock US Patent No. 6,678,833.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 3-5, 7-9, 12-14, and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alexander et al US Patent No. 6,188,602 in view of Grawrock US Patent No. 6,678,833.

With regards to claims 4 and 13, Alexander teaches the receiving of a request to unlock the utility (Alexander, column 5 lines 46-52, operating system requests access to flash), verifying an update to the utility (Alexander, column 5 lines 58-61, verify the data), using a system management interrupt handler to query a status of the verifying step (Alexander, column 5 lines 58-61, smi access state verifies data), and if the

verifying step successfully verifies the update of the utility, unlocking the utility and updating the utility (Alexander, column 5 lines 41-45, if valid RBU image exists allow loading). Alexander fails to teach the verifying being performed by a trusted platform module (TPM) in accordance with the Trusted Computing Alliance Specifications. Grawrock teaches verifying being performed by a trusted platform module (TPM) in accordance with the Trusted Computing Alliance Specifications (Grawrock, column 4 lines 1-9, verification by a challenger). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Grawrock's method of using a trusted platform module because it offers the advantage of allowing the TPM to accurately report the identity of the boot block or utility without reliance on any intervening devices (Grawrock, column 2 lines 1-6).

With regards to claims 3 and 12, Alexander as modified teaches the step of not unlocking the utility if the verifying step fails to verify the update to the utility (Alexander, column 5 lines 34-42).

With regards to claims 5 and 14, Alexander as modified teaches the SMI handler used to query the status of the verifying step queries the TPM for status (Alexander, column 5 lines 58-61, Grawrock, column 4 lines 1-9).

With regards to claims 7 and 16, Alexander as modified teaches the locking of the utility with the SMI handler after the utility has been updated (Alexander, column 5 lines 62-64).

With regards to claim 8, Alexander as modified teaches the utility being a flash utility (Alexander, column 5 line 61, flash memory).

With regards to claims 9 and 17, Alexander as modified teaches the requesting step being performed by an SMI handler (Alexander, column 5 lines 58-62, receiving a request).

With regards to claim 18, Alexander teaches a processor (Alexander, column 2 lines 56-57), a BIOS utility stored in flash memory coupled to the processor (Alexander, column 3 lines 45-46), input circuit for receiving an update to the BIOS utility (Alexander, column 5 lines 11-13), a bus system for coupling the input circuit to the processor (Alexander, column 3 lines 6-24), a BIOS update application requesting an unlock of the flash memory from a system management interrupt (SMI) handler (Alexander, column 5 lines 58-61), the SMI handler unlocking the flash memory if the SMI handler sets the status as successful (Alexander, column 5 lines 58-61 and 42-46), the BIOS update application updating the BIOS utility with the update (Alexander, column 5 lines 42-46), and the SMI handler locking the flash memory after the update of the BIOS utility has completed (Alexander, column 5 lines 62-64). Alexander fails to teach the use of a trusted platform module (TPM) and the requesting of cryptographic verification of the BIOS. Grawrock teaches a trusted platform module coupled to the processor and operating under the Trusted Computing Platform Alliance Specifications (Grawrock, column 3 lines 50-57, column 1 lines 24-36), the requesting of cryptographic verification of the BIOS utility update from the TPM (Grawrock, column 3 lines 1-18, hash operation, boot block identifier), the TMP including programming for issuing an SMI to query the TPM for a status on the verifying of the authenticity of the BIOS utility update (Alexander, column 5 lines 58-61, Grawrock, column 4 lines 1-9). At the time

the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Grawrock's TPM with Alexander's memory device because it offers the advantage of allowing the TPM to accurately report the identity of the boot block or utility without reliance on any intervening devices (Grawrock, column 2 lines 1-6).

(10) Response to Argument

In the instant appeal brief, Applicant has presented the following arguments:

1. On page 5, Applicant has alleged that there is a lack of motivation for the combination of Grawrock and Alexander.

2. On page 5, Applicant has alleged that Grawrock teaches away from the present invention.

3. On page 6, Applicant has alleged that the combination of Grawrock and Alexander fail to teach the SMI handler being used to query the status of the verifying step by querying the TPM for such status.

4. On page 6, Applicant has alleged that the Alexander reference fails to teach "if the verifying step successfully verifies the update of the utility, unlocking the utility and updating the utility" by specifically focusing on an alleged lack of teaching for the "unlocking" step.

1. Motivation for combining Grawrock and Alexander

Applicant has alleged that the Alexander reference does not provide any teaching or suggestion regarding a need for a TPM as taught by Grawrock. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, motivation for the combination can be found in the Grawrock reference. As noted in the prior office actions, Grawrock's TPM provides the advantage of allowing the accurate reporting of the identity of a boot block or utility without reliance on any intervening devices (Grawrock, column 2 lines 1-6). Grawrock's TPM also provides the further advantage of allowing for the detection of modifications to information regarding the boot process originating from the boot block or replacement of the ROM itself (Grawrock, column 1 lines 43-49). This is a distinct advantage over previous systems because updates to a boot block can be verified instead of previous systems where only the original boot block is verifiable. Thus, Examiner maintains that the Grawrock reference provides ample motivation for the combination of Alexander and Grawrock and as a result the combination is proper.

2. Grawrock Does Not Teach Away From the Present Invention

Applicant has asserted that Grawrock teaches away from the present invention. Applicant has cited as evidence Grawrock column 2 lines 1-6 where Grawrock states that the TPM accurately reports the identity of the boot block *without reliance on any intervening devices.* Applicant alleges that the fact that no intervening devices are necessary teaches away from the present invention because Applicant alleges that the present invention as claimed requires an intervening device: the claimed SMI handler (see claim 4 lines 5-6). Examiner respectfully disagrees that the cited portions of Grawrock teach away from the present invention. An SMI handler is not a "device"; it is a special routine that is executed when a specific interrupt occurs (Microsoft Computer Dictionary 5th edition). Applicant's specification is consistent with this definition. The specification states, "after the initial processor state is saved, CPU begins executing an SMI handler routine" (Specification, page 9 lines 15-16). Thus, the SMI handler as disclosed by Applicant is not a separate device, but is instead a piece of software that is executed by a CPU. It is the CPU of the present invention that communicates with the TPM (see Figure 3, Items 410 and 451).

As further evidence that the Grawrock reference does not teach away from the present invention, Examiner notes that Grawrock's TPM operates in the exact same manner as the TPM in the present invention. In the present invention, the TPM responds to a request for verification from an SMI handler being executed on a CPU (Specification, page 9 lines 25-26, Appeal Brief page 5). According to Applicant, this is in essence an intervening device querying the TPM (Appeal Brief, page 5). Examiner

contends this is nothing more than a CPU requesting verification from the TPM. Grawrock's TPM operates in an identical manner. Grawrock discloses a TPM that responds to a request for verification from a challenger. Grawrock defines a challenger as any electronic device within the platform or even external to the platform (Grawrock, page 4 lines 9-14). Thus, Grawrock does teach the use of an intervening device by the definition provided by Applicant and in view of the identical operating nature of the TPM in Grawrock and the TPM in the present invention, Examiner asserts that Grawrock does not teach away from the present invention.

3. Grawrock and Alexander teach the SMI Handler Querying the Status of the Verifying Step.

Applicant has argued on pages 5-6 that Grawrock and Alexander fail to teach the SMI handler being used to query the status of the verifying step by querying the TPM for such status. Examiner respectfully disagrees. Alexander teaches using a system management interrupt handler (SMI handler) to query a status of the verifying step (Alexander, column 5 lines 58-61, smi access state verifies data). Grawrock teaches the TPM responding to a query of the status of a verifying step (Grawrock, column 4 lines 5-19, TPM responds to inquiry requests from a challenger). Thus, a combination of Alexander and Grawrock would teach Grawrock's TPM responding to a request for the status of the verifying step from Alexander's SMI handler (Alexander, column 5 lines 58-62, Grawrock, column 4 lines 10-18). The motivation for such a combination is

provided within the references (as noted above in section 1 of response to arguments). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Grawrock's method of using a trusted platform module because it offers the advantage of allowing the TPM to accurately report the identity of the boot block or utility without reliance on any intervening devices (Grawrock, column 2 lines 1-6) and because it would provid the further advantage of allowing for the detection of modifications to information regarding the boot process originating from the boot block or replacement of the ROM itself (Grawrock, column 1 lines 43-49).

4. Grawrock and Alexander Teach the Claimed Verifying Step

Applicant has alleged that the Alexander reference fails to teach "if the verifying step successfully verifies the update of the utility, unlocking the utility and updating the utility" by specifically focusing on an alleged lack of teaching for the "unlocking" step. Examiner respectfully disagrees. Alexander teaches if the verifying step successfully verifies the update of the utility (Alexander, column 5 lines 60-62, verify the data before unlocking the flash memory) unlocking the utility and updating the utility (Alexander, column 5 lines 60-62, unlock flash memory, see also Figure 3A items 332, 334, 336). Thus, the unlocking step of Alexander (Alexander, column 5 lines 60-62) depends upon a successful verification of the update of the utility (Alexander, column 5 lines 58-67 and 41-45, verifies the RBU image and then unlocks memory to allow flashing the memory, flashing the memory replaces the old data with the new).

Applicant furthers this argument by alleging that the combination of the references fails to teach that an update to one of these software modules is performed by the TPM before an update of such software module is accomplished (Appeal brief, page 6). Specifically, Applicant argues that Grawrock teaches verification after the update has already been loaded onto the system and Applicant alleges that the present invention provides a way to verify the BIOS is unaltered before it is allowed to be flashed onto the system. Applicant appears to be using the words "loading" and "flashed" interchangeably. Loading a utility may include loading a utility into the memory of a system, but does not necessarily mean replacing the utility with a new updated utility. Flashing a utility means replacing the utility with a new updated utility permanently in flash memory. As noted in the Final Office Action, Examiner has relied upon Alexander for this feature. Alexander teaches that if an RBU exists (Alexander, column 5 lines 9-18, RBU being an update to the utility as claimed), verifying the RBU (Alexander, column 5 lines 57-67), and then flashing the RBU into memory thus replacing the utility (Alexander, column 5 lines 60-62). Thus, contrary to Applicant's assertion, Alexander and Grawrock teach verification of the utility before it is allowed to be flashed onto the system. Further, as noted in the Final Office action, the claims as currently presented do not provide any limitations preventing the loading of a new utility onto the system before verification. Instead, the claims only prevent the updating of the utility until the utility is successfully verified (see Claim 4 lines 10-12, if verifying step successfully verifies the update of the utility...updating the utility). Alexander teaches

preventing the updating of the utility until the utility is successfully verified as shown above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Andrew Nalven ALN

Conferees:

Gilberto Barron

Matthew Smithers

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137